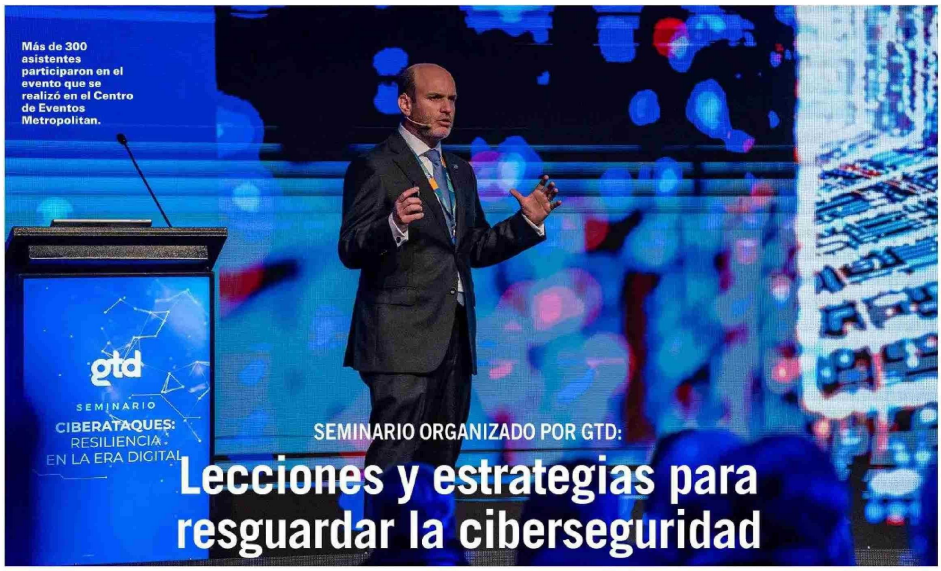
LITORALPRESS

Fecha: 29-06-2024
Medio: El Mercurio
Supl. : El Mercurio - Chile Tecnológico
Tipo: Noticia general
Título: **“Lecciones y estrategias para resguardar la ciberseguridad**

Pág. : 9
Cm2: 1.017,4

Tiraje: 126.654
Lectoría: 320.543
Favorabilidad: No Definida

CONTENIDO PATROCINADO



SEMINARIO ORGANIZADO POR GTD:

Lecciones y estrategias para resguardar la ciberseguridad

En el evento “Ciberataques: Resiliencia en la era digital”, Gtd compartió los aprendizajes clave tras el ataque que sufrió en 2023; entre ellos, la colaboración con aliados y autoridades, la comunicación transparente con los clientes y la necesidad de una cultura resiliente en seguridad cibernética.

“Existen tres tipos de compañías: las que ya han sido atacadas, las que están siendo atacadas y las que serán atacadas en el futuro”, dijo Fernando Gana, gerente general de Gtd, en el seminario “Ciberataques: Resiliencia en la era digital”, organizado por la empresa de tecnología y telecomunicaciones.

En el evento, se presentaron los principales aprendizajes derivados del ciberataque detectado el 23 de octubre de 2023.

Con la certeza de que mañana puede ser cualquiera, Gana explicó los tres aprendizajes clave del incidente. El primero, trabajar de manera colaborativa con los clientes, las autoridades, los aliados, los colaboradores y cualquier persona dispuesta a ayudar. “En un ciberataque, nos enfrentamos a un enemigo común: los ciberdelincuentes. Necesitamos trabajar juntos contra ellos”, afirmó.

Tras el ataque, Gtd informó de inmediato al CSIRT de gobierno y a la Subtel. Además, se notificó a los clientes para que activaran sus protocolos de emergencia y aseguraran la continuidad de sus operaciones.

El gerente general resaltó la importancia de tener un socio tecnológico confiable durante las crisis; la compañía contaba con SecureSoft, el Centro de Excelencia en ciberseguridad de Gtd. Además, destacó la contribución de empresas externas expertas como Microsoft Dart, Mandiant de Google y Dell en la formulación de nuevos protocolos de recuperación. “Las terceras visiones son relevantes al tomar decisiones”, expresó.

CULTURA RESILIENTE

El segundo aprendizaje que mencionó el gerente general de Gtd es comunicar con integridad y transparencia. “Aunque inicialmente teníamos muy poca información, nos enfrentamos a preguntas cruciales: ¿Comunicamos ahora a nuestros clientes? ¿Qué comunicamos? ¿Esperamos a tener más información?”, comentó.

“Desde el primer momento, nos comprometimos a mantener una comunicación continua y constante, tanto para informar buenas noticias como encontrar equipamiento, como malas noticias”, añadió.

El tercer aprendizaje había sido compartido en el seminario “Construyendo una cibercultura resiliente”, realizado en agosto de 2023, donde presentaron cuatro focos importantes para mantener una cultura resiliente en la ciberseguridad. Primero, crear conciencia a través de la educación y capacitación, para que las personas no sean víctimas de engaños de delincuentes. Segundo, desarrollar habilidades técnicas y contar con soporte adecuado para prevenir y detectar amenazas. Tercero, implementar un plan de respuesta a incidentes conocido por toda la compañía. Cuarto, mantenerse actualizado mediante una inversión constante en ciberseguridad, ya que “la prevención, la detección, la reacción y la recuperación son fundamentales. Sin embargo, es crucial enfocarse en la recuperación de los servicios de manera eficaz y eficiente”.

Después de la experiencia vivida surgió un quinto foco: la confianza y liderazgo del equipo.

Para enfatizar, se entregó un cuestionario sobre decisiones a tomar frente a un ataque. ¿Sabes cómo tu empresa lo enfrentaría? ¿Cómo impactaría a tus colaboradores y clientes? ¿Sabes a qué autoridades notificar? ¿Puedes operar desconectado más de 24 horas? ¿Tu equipo está empoderado para tomar decisiones difíciles con muy poca información? ¿Sabes cómo gestionar una crisis así?

Este seminario fue posible gracias al apoyo de aliados como Cisco, Dell Technologies, Microsoft, Fortinet, Huawei, Ingram-HPE Aruba, Watchguard, Vmware, Veeam, TD Synne-IBM y Acronis.

CONFIANZA EN LOS DATOS

La IA aporta beneficios a la ciberseguridad, pero para evitar malos entendidos y ganar la confianza de los usuarios, Microsoft ha establecido principios responsables con un enfoque en la confiabilidad de los datos, dice Brad Ligget, panelista internacional y experto en ciberseguridad de Microsoft.

Con una conexión API, se puede verificar la veracidad de la información. Luego, se envía un *prompt* modificado al modelo de lenguaje (LLM). Este genera la respuesta basada en la pregunta original y esa respuesta se procesa en Azure OpenAI, manteniendo la confianza en la seguridad de Microsoft.

“Aplicamos rigurosamente los principios de IA responsable, cruzamos y verificamos los datos, asegurándonos de que la respuesta del LLM sea adecuada antes de devolverla al usuario de la pregunta original”, afirma.

LA CIBERSEGURIDAD COMO UN TODO

En el top 4 de los riesgos globales, según el *ranking* del World Economic Forum, se encuentran la desinformación, el clima extremo, la polarización social y la ciberinseguridad.

“Estos riesgos están interconectados y no deben considerarse elementos aislados. La ciberinseguridad facilita la generación de información falsa, lo que conduce a la desinformación, que provoca polarización social”, dijo Juan Marino, *regional sales manager* de Ciberseguridad de Cisco, durante su intervención en el seminario “Ciberataques: Resiliencia en la era digital”.

Ante la amenaza del cibercrimen, han surgido más de tres mil fabricantes de seguridad cibernética que buscan resolver este problema. Sin embargo, este mercado “caótico” da lugar a un “falso profeta”: vender soluciones que pueden no ser lo que verdaderamente se necesita.

Por eso, existe el “ABC de la ciberseguridad”, con cinco funciones clave en relación con ella, afirmó Marino. La primera es identificar lo que se quiere proteger, ya que “sin identificación no se puede proteger”.

La segunda es la prevención, mediante una serie de controles que, aunque necesarios, no son suficientes por sí solos.

La tercera es la detección, que implica tener las capacidades y procedimientos para identificar posibles amenazas. Una vez detectadas, la cuarta función es responder, activando un protocolo para manejar las amenazas que no pudieron ser prevenidas ni bloqueadas.

Finalmente, un principio fundamental es asumir que los incidentes ocurrirán. Por ello, además de responder, hay que estar preparados para lidiar con las consecuencias y ser capaces de recuperarse de ellas. Este es el ciclo completo de la ciberseguridad.

Recientemente se incorporó un elemento transversal que, aunque intrínsecamente presente en las cinco funciones, necesitaba más entidad: el gobierno de la ciberseguridad. La estrategia de seguridad cibernética debe atravesar estas cinco dimensiones y configurar una matriz de 5x5, con los cinco aspectos a proteger: dispositivos, redes, aplicaciones, datos e identidades de los usuarios.

“De los 3.000 fabricantes de ciberseguridad, la mayoría solo resuelve una pequeña parte del problema”, explicó Marino. “Pero no se puede construir una estrategia de ciberseguridad efectiva combinando 20 productos de 20 fabricantes. La respuesta parece ser la consolidación: una plataforma integral que proteja todas las dimensiones necesarias, evitando la complejidad de conectar múltiples productos distintos”.

Hoy, Gtd es más fuerte y está mejor preparada para enfrentar este tipo de incidentes gracias a las lecciones aprendidas”.

FERNANDO GANA,
gerente general de Gtd.

Solo el 3% de las empresas del mundo tiene el nivel de preparación para resistir riesgos de ciberseguridad modernos”.

JUAN MARINO,
regional sales manager de Ciberseguridad de Cisco.

Queremos ayudar a los equipos de seguridad a operar eficazmente para neutralizar a los adversarios”.

BRAD LIGGET,
experto en Ciberseguridad de Microsoft.